Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

| TRANSMITTAL SLIP | DATE 1/23/86 |
|---|---|
| TO: DDCI | |
| ROOM NO. | BUILDING |
| REMARKS: FYI<br>→ D/OLL<br>FYI<br>Dianne<br>1/23/86 | |
| FROM: | |
| ROOM NO. | BUILDING / EXTENSION |

FORM NO. 1 FEB 56 241 REPLACES FORM 36-8 WHICH MAY BE USED. (47)

DDCI Copy Given to OLL
23 JAN. 86

DCI EXEC REG

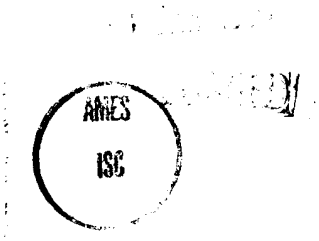
B-602-IR

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

SECRET

D/ICS-86-0767
17 January 1986




MEMORANDUM FOR: Distribution

FROM: Richard G. Stilwell
Chairman, SIG-I Working Group

SUBJECT: Counterintelligence Capabilities Improvements Report (U)

REFERENCE: a. Public Law 99-169: Intelligence Authorization Act, FY 1986, Section 402

b. SIG-I Chairman memorandum, 20 December 1985, subject: Counterintelligence Capabilities Improvements Report (U)

The attached correspondence constitutes an orientation on the background, organization, and methodology relating to preparation of the President's report to Congress which has been requested by reference a. The SIG-I Chairman has appointed a representative to oversee preparation of the report, established a working group of SIG-I representatives to develop the report, and assigned staff support responsibility to the Community Counterintelligence Staff, Intelligence Community Staff (reference b). Addressees are requested to review the attached correspondence and support follow-on tasking as required. (U)

Richard G. Stilwell
General, USA (Ret.)

25X1

Regrade Unclassified when separated from classified attachments

SECRET

B-602-IR

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



# COUNTERINTELLIGENCE CAPABILITIES IMPROVEMENTS REPORT

## BACKGROUND

As a result of the several national security incidents occurring in 1985, considerable attention has been focused on US counterintelligence and security countermeasure policies, procedures, and capabilities. A number of executive branch actions were taken and others are in progress. The intelligence oversight committees of Congress began an assessment of US foreign counterintelligence (FCI) and security countermeasure (CM) programs. The Senate Select Committee on Intelligence (SSCI), in particular, has held a series of hearings as input to the report it intends to submit to the Senate on what should be done to improve US CI and CM posture. [redacted] 25X1

There have been four SSCI hearings held thus far. [redacted] 25X1

[redacted] 25X1

This correspondence provides some flavor of the thinking of the SSCI with respect to this entire issue. [redacted] 25X1

The overall impression conveyed is that the SSCI is relatively satisfied with the manner in which the foreign counterintelligence system is functioning.



Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8


Specifically, some "fine tuning" of the foreign counterintelligence structure is indicated in such areas as counterintelligence training, analysis, and enabling legislation. On the other hand, it has become clear that the Committee believes there is inadequate national policy coordination and functional guidance with regard to the security programs and countermeasures designed to protect classified information.

25X1

25X1

25X1



Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8


As reflected in Tab C, the intelligence oversight committees have requested that the President provide a report on counterintelligence/security countermeasures. The SSCI envisions that the substance of that report will be reflected in the document the SSCI will eventually submit to the Senate; there may not be a counterpart HPSCI report to the House. 25X1

25X1



Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

25X1

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Page Denied

Next 11 Page(s) In Document Denied

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

ATTACHMENT A

STATEMENT OF

SENATOR DAVE DURENBERGER, CHAIRMAN
SENATOR PATRICK LEAHY, VICE CHAIRMAN

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

October 22, 1985

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Tuesday, October 22, 1985

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

We appreciate the opportunity to testify before the Permanent Subcommittee on Investigations with regard to the hostile intelligence services threat and the actions required to counter that threat. The Subcommittee has done outstanding work on security issues. The hearings in 1982 on Soviet efforts to acquire American technology helped make the public and the Congress aware of the seriousness of the problem. The hearings on personnel security last spring demonstrated the need for major improvements in security clearance policies. The Select Committee on Intelligence is committed to following up on the recommendations that emerged from those hearings.

We are especially pleased that today's hearing will focus on ways to control the numbers and activities of Soviet and other foreign representatives who conduct espionage and related activities in the United States. The Soviet bloc presence goes far beyond their diplomats in Washington and amounts to some 2,500 positions in embassies, U.N. Missions, the U.N. Secretariat, trade and commercial operations and other offices. Much more must be done to counter the intelligence threat posed by these potential and actual intelligence agents.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Several cases show why the problem goes beyond just Soviet diplomats. In 1983, an employee of the Bulgarian trade office in New York -- a man named Kostadinov -- was arrested for espionage based on evidence that he bought a secret document on security procedures for American nuclear weapons. Kostadinov had been working in the trade office without diplomatic immunity since 1979. A second case involved an American businessman, James Harper, who sold documents from a defense contractor's office on Minuteman missile secrets to Polish intelligence. The key figure who introduced Harper to the Poles was another California businessman, William B. Hugle, whose firm had received large payments from the Polish electronics firm Unitra. The use of commercial cover and business dealings for espionage purposes is documented in other cases, including the Bell case where an employee of a defense contractor was recruited as a spy by an official of the Polish firm Polamco.

FBI Director Webster has said that the cases like Bell and Harper which come to public attention "are merely the tip of the iceberg." The counterintelligence information provided to the Select Committee confirms Judge Webster's statement.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Although the Intelligence Committee does most of its work in closed hearings, we believe it is vital for the entire Senate and the public to be aware of the full dimensions of the espionage problem. For one thing, there is quite a bit that the average citizen can do to strengthen the nation's defenses, especially if the individual works for the federal government, a government contractor, or a high-tech industry or research program. The public also needs to know what we in government are doing about foreign espionage and whether we should be doing something more. For that reason, we plan to make a public report to the Senate at the end of the Select Committee's review of U.S. counterintelligence and security programs.

The subject of today's hearing is a significant element in the comprehensive review of U.S. counterintelligence and secruity programs that the Select Committee is conducting. This open hearing is therefore a good place to give your Subcommittee and the entire Senate a preliminary report on the Select Committee's work. Our report explains the context and importance of some specific recommendations we want to offer, based on the Select Committee's review of the hostile intelligence threat and U.S. countermeasures over the past several years.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



From its inception, the Select Committee has given high priority to counterintelligence concerns. Two of the Committee's first legislative proposals -- the Foreign Intelligence Surveillance Act of 1978 and the Classified Information Procedures Act of 1980 -- have been a significant help to U.S. counterintelligence. Starting with FY 1979, the Intelligence Committee has reviewed the U.S. counterintelligence budget as a whole and taken the lead to increase money and manpower for counterintelligence in the FBI, the CIA, and the Defense Department. The Committee has also looked at the damage done by major espionage cases, some of the deficiencies in personnel and communications security, the value of techniques such as the polygraph, and measures to improve counterintelligence operations and analysis.

At the beginning of the 99th Congress, we decided that one of the Committee's most important tasks under our leadership should be to make an independent assessment of the counterintelligence and security requirements for dealing with Soviet espionage and other hostile intelligence threats. Although we made this decision before the Walker case, it was already clear that espionage arrests were on the increase and that hostile intelligence operations posed a growing problem for national security.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Thus far this year, the Intelligence Committee has held at least seven closed sessions on counterintelligence and security matters. We have considered CI program and budget requirements for FY 1986, the need for greater control over the numbers and activities of hostile intelligence officers in this country, the security situation at the U.S. Embassy in Moscow, the damage done by the Walker espionage network, the requirements for a $35 million supplemental appropriation for security countermeasures at U.S. facilities abroad, and a comprehensive survey by senior FBI and CIA officials of the full extent of the hostile intelligence threat. Most recently, the Committee has had several briefings on the Howard case. We are reviewing the personnel, security, and management procedures associated with this case and other ramifications of the defection of senior KGB official Vitaly Yurchenko, who served in the Soviet Embassy here in 1975-80.

1. The Espionage Problem

The hostile intelligence threat has many facets, and not all of them surface in espionage prosecutions. It is important to consider all the dimensions in developing a national strategy to deal with that threat.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



a. The Human Dimension

The Howard and Walker cases are the latest in a series of major espionage cases that show how vulnerable U.S. national security secrets are to foreign espionage. The expulsion of scores of Soviet agents from France and Britain, the penetrations of the West German Government, and other espionage cases in Norway and Greece indicate the worldwide success of Soviet intelligence operations. As documented in the recent interagency report on Soviet Acquisition of Militarily Significant Western Technology, the Soviets devote massive resources to systematic efforts to penetrate Western governments and high-tech industry.

The Soviets also use other East European intelligence services as surrogates, because they have access to places where Soviets cannot go. The Bell and Harper cases illustrated the effectivenesss of Polish intelligence in penetrating U.S. defense industries. In the Harper case, top Soviet intelligence officials came to Warsaw to get the information on U.S. missile defense systems. East German agents arrested in the United States over the past two years include a woman courier in an espionage network and a prominent scientist attempting to recruit American scientists.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



At a closed hearing last July, the FBI told the Select Committee that the espionage cases of the last two years have involved billions of dollars of actual and potential damage to U.S. military programs. The problem is compounded by the vast number of Chinese officials and visitors in the U.S. While U.S.-PRC relations are good, there is clear evidence of clandestine intelligence operations by the Chinese in the United States. These activities greatly increase the burden on the FBI's counterintelligence resources.

An Intelligence Community study summarizes the human threat in the following terms:

> Despite the development of increasingly sophisticated technical means of intelligence collection, the human agent continues to be the most important key to satisfying a nation's intelligence needs. The Communist countries depend to a large degree on their human collection networks throughout the world to satisfy their U.S.-related intelligence requirements -- requirements ranging from acquisition of advanced technology, location and determination of the quality of strategic and conventional military forces, and assessment of U.S. reaction to international political incidents, to discovery of techniques used by U.S. counterintelligence. A major, highly structured effort is dedicated to the acquisition of U.S. cryptographic information and materials that would allow the exploitation of secure U.S. communications. Success in this area can fulfill many of the requirements mentioned above.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



b. The Technical Threat

Electronic espionage is as serious as the human variety. The Soviets listen to our telecommunications from their diplomatic establishments, from ships off our shores, and from a sophisticated monitoring site at Lourdes, Cuba, that can intercept our domestic and international satellite communications channels. While the most sensitive data are encrypted, the Soviets can exploit uncoded communications that deal with sensitive military, scientific, and economic developments. If communications security is lax, they can also get classified data. In 1978, a Soviet diplomat defected to the United States and said that telephone and telex calls were monitored at the Soviet recreational facility in Glen Cove, New York, which required the shipment of tons of material to Moscow annually. Satellite communications are potentially an extremely valuable source of information as they can simultaneously transmit thousands of telephone, T.V., and computer-to-computer transactions. The explosion in computer networks and the electronic transfer of data adds another major area for Soviet exploitation.

Computers and office equipment are also vulnerable to the most sophisticated electronic penetration and eavesdropping techniques. The reported discovery of bugged typewriters

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



at our Moscow Embassy illustrates the Soviets' impressive technical surveillance capabilities. Part of the problem is physical security, because the Soviets should never have gotten access to Moscow Embassy equipment.

Technical and human threats are inextricably linked. When foreign nationals employed at our embassies abroad can get access to sensitive offices or equipment, the chances for bugging greatly increase. At the same time, foreign nationals working in our embassies can assess the weaknesses of American employees on behalf of hostile intelligence services for possible recruitment. Here in this country, the human vulnerabilities that produce a Howard, a Walker, a Harper, or a Bell can given the Soviets not only specific facts and documents, but also codes and access to computer data systems that multiply the damage enormously.

c. Seeking A Balanced Response

The Select Committee is seeking to identify, in concert with the Executive branch, those actions that can be taken to improve U.S. counterintelligence and security protections without departing from our nation's basic principles.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



In espionage, as in terrorism, there is a risk of overreaction that sacrifices individual rights and the rule of law for the sake of security.

Protection of national security secrets is not easy in a free society. Total preoccupation with security -- to the exclusion of other values -- would undermine the constitutional principles that America stands for throughout the world. If we seek to copy the secret police methods of our adversaries, they will have won a great victory. If, however, we show that the United States can protect its security without sacrificing fundamental freedoms, the essential superiority of an open society will be vindicated.

As President Reagan said in a nationwide radio address on June 29, 1985:

> "[W]e can counter this hostile threat and still remain true to our values. We don't need to fight repression by becoming repressive ourselves.... But we need to put our cleverness and determination to work and we need to deal severely with those who betray our country. We should begin by realizing that spying is a fact of life and that all of us need to be better informed about the unchanging realities of the Soviet system.... There is no quick fix to this problem. Without hysteria or finger pointing, let us move calmly and deliberately together to protect freedom."

Some proposals offered in the name of security may even be counterproductive. Closing down channels for the open exchange of unclassified basic scientific research

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



could do immense damage to the system of free scientific inquiry that keeps America so far ahead of the Soviets. The recent interagency report on Soviet acquisition of Western technology warned that restricting access to unclassified scientific data "may also inhibit the United States' own national research effort." Similarly, rapid expansion of the use of lie detector tests without the most careful quality controls and training for polygraph examiners not only could harm employee morale by treating individuals unfairly, but also could create a false sense of security and prevent other steps necessary to ensure the reliability of people in sensitive jobs.

2. Select Committee Study

On June 11, 1985, the Select Committee announced that it would conduct a comprehensive review of the Soviet intelligence threat and U.S. counterintelligence and security programs, including an examination of the implications for national security of the Walker espionage case. From the outset, our guiding principle has been to cooperate with the Executive branch in this effort. We have worked closely with the National Security Council staff and the relevant agencies and departments, and we expect that the President will shortly select a senior official to represent the

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Administration at a series of closed hearings on all aspects of counterintelligence and security. The objective is to reach agreement with the Administration on a common agenda for immediate actions and long-range decisions.

The closed hearings we have scheduled for this fall are planned to provide an overview of Administration actions on counterintelligence and security, including recent decisions and topics under review. We expect to take a close look at technical counterintelligence and security, at the long-range plans and requirements for counterespionage into the 1990s, at personnel and information security policies, and at the relationships between counterespionage and foreign policy. Much of our attention is focused on the adoption and implementation of recommendations that have already been made by other bodies, including the proposals made on June 6, 1985, by the Chairman and Ranking Minority Member of the Permanent Subcommittee on Investigations after hearings on security clearance programs last spring.

In preparation for our hearings, the Committee staff has conducted over fifty interviews with government officials and outside experts across the full spectrum of intelligence, military, diplomatic, industrial, and security fields. The staff has also pulled together the record of legislative and administrative actions in recent years.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Most important of all, the Committee is compiling the results of a series of important studies of counterintelligence and security matters that have been conducted within the Executive branch. We also await the completion of two significant studies that are currently underway. The first is the report of the DoD Security Review Commission, chaired by General Richard G. Stilwell, the former Deputy Under Secretary of Defense for Policy. The Stilwell Commission has been charged with the task of identifying any "systematic vulnerabilities or weaknesses" brought to light as a result of the Walker case and making recommendations for changes to correct those deficiencies. The second study will come from an interagency task force headed by the Director of the Information Security Oversight Office, Steven Garfinkel, which is developing recommendations for a systematic attack on the problems of overclassification and overdistribution of sensitive information.

Based on these and previous Executive branch studies, the Select Committee's own closed hearings, and our ongoing dialogue with Administration officials, we hope to reach agreement on specific administrative and legislative actions that will have the joint support of the President and the Select Committee.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



The Select Committee is also reviewing its own security procedures and those of the Senate as a whole. In July, the Committee offered its services to other Senate offices as a focal point for security briefings and advice. The Committee has implemented new security measures internally and will work with the Sergeant at Arms and other appropriate officials to improve security for all of us in the Senate.

3. Administrative and Congressional Initiatives

We need to identify what has already been accomplished in order to decide what more needs to be done. Concern about Soviet espionage and the need to improve U.S. countermeasures is not new, even though greater public attention has focused on the problem this year. Recent Administration initiatives have included:

-- Establishment of a policy review structure under the National Security Council for counterintelligence requirements and a small Community Counterintelligence Staff drawn from the FBI, CIA, and DoD to prepare national assessments of the hostile intelligence services threat and U.S. countermeasures.

-- The Foreign Missions Act of 1982, which created a new Office of Foreign Missions in the State Department to exercise greater control over the activities of foreign officials in this country. Under the able leadership of its Director, former FBI counterintelligence official James E. Nolan, the Foreign Missions Office has used this authority to enhance U.S. security within the framework of diplomatic reciprocity.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



-- NSDD-145 on telecommunications and automated information systems security, issued by the President in 1984 to promote the development of coherent, long-range plans for improving U.S. communications and computer security.

-- Defense Department actions this year to reduce the number of security clearances, to enforce need-to-know limits on access to particular programs or activities, to tighten procedures for granting clearances, and to require that supervisors evaluate the security performance and reliability of cleared personnel.

-- A Presidentially-ordered five-year buildup of FBI foreign counterintelligence resources, which began in 1983 and has had full Congressional support in the annual Intelligence Authorization Acts.

-- Substantial increases in funding for the counter-intelligence programs of the military services and DIA, whose budgets are consolidated in the DoD Foreign Counterintelligence Program managed by the office of the Deputy Under Secretary of Defense for Policy. These increases have also had full support in the Intelligence Authorization Acts.

These Administration actions have made progress, but as the President emphasized in his June 29 address, much more must be accomplished.

In several areas, Congressional action has been taken to encourage or facilitate specific countermeasures:

-- The Huddleston-Leahy amendment to the Intelligence Authorization Act for FY 1985 requires annual reports to the Intelligence and Foreign Relations Committees on steps taken to reduce the disparities in numbers and treatment between officials in the United States from countries that engage in hostile intelligence activities and U.S. officials in those countries.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



-- The Leahy-Cohen amendment to the State Department Authorization Act for FY 1986 establishes the policy that the numbers of U.S. and Soviet embassy and consular personnel should be substantially equivalent, unless the President makes an exception, and requires that a plan to achieve equivalence be submitted by February, 1986.

-- The Roth amendment to the State Department Authorization Act for FY 1986 authorizes the State Department to regulate the activities of U.N. Secretariat personnel and requires that such personnel be subject to the same controls as diplomats from their home country, unless the requirement is waived by the Secretary of State.

-- The Durenberger-Leahy amendment to the FY 1985 Supplemental Appropriations Bill provides $35 million to enhance security countermeasures at U.S. Embassies and other facilities abroad.

-- The State Department Authorization Act for FY 1986 calls for replacing Soviet employees at our Moscow Embassy with Americans to the extent practicable.

-- The Statement of Managers accompanying the Conference Report on the State Department Authorization Act for FY 1986 calls for a report on illicit electronic surveillance in the United States by foreign governments.

In addition to these measures already enacted, the pending Conference Report on the Defense Department Authorization Act for FY 1986 includes provisions offered by Senator Nunn to add funds for reducing the security clearance backlog, to require Presidential guidance and a report on personnel security policy, and to give DoD background investigations a

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



conditional exemption from OPM regulations. The pending defense bill also contains a new article in the Uniform Code of Military Justice permitting the death penalty for espionage in certain circumstances, a requirement for a report on the desirability of reinstituting the death penalty for civilian espionage, and limits on the "test program" for expanded use of polygraph examiniations in DoD so as to ensure quality controls and prevent mistakes. The conference on the Intelligence Authorization Act for FY 1986 is considering Senate provisions to increase Defense Department access to to criminal records for employee security background checks and to facilitate military counterintelligence double agent operations, as well as a House proposal for a DCI report on security vulnerabilities abroad.

While individual Senators may have differing views on one or another of these actions, the record clearly demonstrates a vigorous and determined effort by the Congress to address serious problems.

4. A Strategic Approach to Counterintelligence and Security

This list of Administration and Congressional initiatives hardly scratches the surface of the numerous recommendations for counterintelligence and security improvements that

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



have been made by various recent studies, mainly within the Executive branch. The Select Committee has been reviewing these proposals with Administration officials so as to arrive at a common agenda. It is increasingly clear that a strategic framework is needed for deciding where to concentrate. Thus far, both the Administration and the Congress have addressed these issues piecemeal. Many different agencies and Congressional committees have taken up parts of the problem, but nowhere has anyone tried to pull all the elements together in one place for a comprehensive assessment.

Recognizing this vacuum, the Select Committee has begun exactly that kind of systematic review. The Select Committee has had the benefit of some of the best thinking in the government as we work with Administration officials to reach agreement on the essential elements of a national strategy.

a. A National Counterintelligence Strategy

We believe we are close to an agreement, based on statements of the President and our consultations with key NSC officials, that the Executive branch should develop a national counterintelligence strategy. We are making a distinction here between "counterintelligence" measures and "security" programs. The best way to explain the difference

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



is to say that counterintelligence measures deal directly with hostile intelligence service activities, while security programs are the indirect defensive measures that minimize vulnerabilities.

From this perspective, a national counterintelligence strategy is not limited to the FBI, CIA, and DoD agencies that carry the "counterintelligence" label. It also includes those diplomatic and regulatory policies that control the numbers and movements of hostile intelligence service officers in this country and at U.S. facilities abroad. Each year, in the formal classified justification for funds for its Foreign Counterintelligence Program, the FBI advises Congress that, even with increased resources, the FBI cannot cope with the hostile intelligence threat unless measures are also taken to reduce the number of potential intelligence officers in this country. Where the numbers cannot be reduced, controls on their movements can assist the FBI in making better use of limited resources.

The organizational structure is already in place to develop and implement a national counterintelligence strategy. The relevant NSC committees and the Community CI Staff can provide the necessary forum for policy development, planning, and oversight of implementation. The Presidential

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



mandate is also clear. In his address of June 29, the President said the Administration had "developed a list of things to be accomplished in the counterintelligence and security areas." He said he was "tasking Cabinet officers to implement the improvements and reforms... on a priority basis." The areas mentioned by the President were;

-- Better means for informing the public about the Soviet intelligence threat.

-- Reduction of the size of the hostile intelligence presence in the U.S. from the present level of more than 2,500 Soviet bloc officials.

-- Establishing "a balance between the size of the Soviet diplomatic presence in the United States and the U.S. presence in the Soviet Union."

-- Better controls on "foreign intelligence agents working at the U.N. who have utilized that organization as a spy nest."

-- Improvement of U.S. counterintelligence capabilities, including "better coordination between counterintelligence agencies, better analysis of hostile threats" and adequate legal authority.

The basic question is whether the Executive branch will implement these measures (and other, classified actions) in the face of opposition from elements that have a vested interest in leaving things the way they are. In some areas, legislation may be required to implement fully the President's national counterintelligence strategy. In other areas, bureaucratic inertia must be overcome. The

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Select Committee on Intelligence stands ready to help with both processes.

b. A National Strategic Security Program

On the security side, we are discussing with the Administration the desirability of formulating a National Strategic Security Program. The government today does not have a comprehensive and integrated security program to protect the information and activities that have the greatest strategic importance to the United States. Such a program would develop national policy direction and guidance and oversee policy implementation for:

- Personnel security
- Information security and classification
- Telecommunications, computer, and other technical security
- Physical security
- Industrial security
- Interrelationships among these elements
- Research and development efforts
- Security awareness requirements

To assist the National Security Council, there should be a structure for long-term planning and systematic analysis of all aspects of strategic security. It should be a focal point for the various overlapping forums that now divide responsibility for security policy.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



This is not a new proposal. Almost thirty years ago, the Congress established a Commission on Government Security with members appointed by the President and the Congressional leadership. Its chairman was a former President of the American Bar Association, and the Vice Chairman was Senator John Stennis. In its 1957 report, the Commission called for a Central Security Office to ensure greater uniformity and higher quality for personnel and industrial security throughout the government. The Commission also stressed "the dangers to national security that arise out of overclassification of information which retards scientific and technological progress" -- and proposed abolishing the Confidential classification because the danger of access to such material was "not significant" and the clearance requirements afforded "no real security-clearance check." The passage of nearly thirty years has not diminished the relevance of these recommendations.

Among the options we expect to see emerge from the Stilwell Commission is an improved personnel security system for those positions with access to information or activities of the greatest strategic importance. We will need to consider more stringent requirements for such

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



positions, including regular financial reports; prior notice of all foreign travel; high personal reliability standards with enforcement by superiors; a clearance policy that selects the most qualified personnel, rather than merely weeding out the worst; and a strong inspection system. It may also be necessary to consider legislation to apply to such positions post-employment obligations and perhaps revised criminal penalties.

These are examples of specific ideas that are being considered as part of the agenda for immediate actions and long-term decisions to strengthen U.S. strategic security. In addition, when we proposed what became the $35 million FY 1985 supplemental appropriation for security countermeasures abroad, we asked the DCI to plan how to use those funds in the context of a long-range strategy for dealing with hostile intelligence threats to U.S. facilities overseas. There may well be merit in proposals to institute a "systems security budget" for telecommunications and information systems security in order to coordinate U.S. Government efforts to influence private industry to undertake the development and production of more secure equipment and systems. And a better balance is needed between high-cost research on technical security projects and the current

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



inadequate funding for research on personnel security. The most secure hardware and software are no guarantee against a Walker, a Bell, or a Harper who decides to sell out his country. When security countermeasures against Soviet espionage are assessed in a single forum, the significance of such gaps becomes clearer and innovative policy may result.

5. Recommendations to Limit the Hostile Intelligence Presence

The importance of limiting the hostile intelligence presence in the United States should be obvious to everyone. Nevertheless, foreign policy considerations and perhaps legal obstacles have inhibited the Executive branch for many years from taking reasonable steps to make it more difficult for hostile intelligence services to operate inside this country. Creating a less favorable environment for espionage operations inside the United States should be the foundation of a national strategy. While we are still considering various proposals for improving the capabilities of the FBI and other U.S. counterintelligence agencies and for improved security measures, four recommendations deserve immediate attention. Each is fully consistent with the President's stated goals and should be implemented by the Executive branch unless there are legal obstacles requiring new legislation.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



a. Equivalence in U.S.-Soviet Embassy/Consular Personnel

The Leahy-Cohen amendment establishes a policy of, in the words of the President on June 29, requiring "a balance between the size of the Soviet diplomatic presence in the United States and the U.S. presence in the Soviet Union." Some State Department officials appear to believe that this balance should be achieved solely by increasing the number of Americans in Moscow, to replace Soviet nationals employed at our Embassy. This totally misreads the intent of Congress and conflicts with the President's policy. While replacing Soviet nationals with Americans in Moscow will help improve security at the Embassy, it need not be done wholesale. Equally, if not more important, is a gradual reduction in Soviet personnel in the United States, as the President made clear when he said "we need to reduce the size of the hostile intelligence threat we're up against in this country." In determining equivalence, it is vital to ensure that we count all the Soviets employed at their embassy and consulates, and not just those on the official diplomatic list.

b. Reducing the Size of the Soviet U.N. Mission

Besides Soviet embassy and consulate personnel, the

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



largest number of Soviet officials in the United States are assigned to the Soviet Mission to the United Nations (SMUN). That is the next place to cut in achieving the President's goal of making a significant reduction in the 2,500 Soviet bloc officials in this country. The SMUN is more than twice the size of any other country's U.N. mission -- the next largest being the U.S. and Chinese missions. It should be possible for the United States to insist on the principle of equivalence as the base-line for reaching agreement with the U.N. on the size of the SMUN. This reduction in the number of potential intelligence officers would make a significant difference as far as the FBI's counterintelligence burden in New York City is concerned. It is not hard to imagine the enormous difficulties that confront the FBI in covering the activities of possible intelligence officers in a place like Manhattan.

c. Foreign Missions Office Controls on Warsaw Pact Country Representatives

Although the State Department has restricted travel in the United States by Soviet officials, placing some areas off limits and requiring Soviet officials to make travel arrangements through the Foreign Missions Office, similar

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



controls have not been placed on officials of other Warsaw Pact countries. Yet there is overwhelming evidence that the Soviets use the intelligence services of Warsaw Pact countries as surrogates. The recent report on Soviet Acquisition of Militarily Significant Western Technology documents these relationships fully. It reflects the Intelligence Community's judgment that the Soviets are likely to intensify their efforts by "increasing their dependance on surrogates among the East European intelligence services." The report also notes that one of the reasons for the "considerable success" of East European services is that "they operate under less severe travel restrictions" than do the Soviets. Given the evidence of this growing threat, the State Department should at least require Warsaw Pact country representatives to make travel arrangements through the Office of Foreign Missions. Moreover, if the FBI detects officials or representatives of a Warsaw Pact nation engaging in espionage-related activities in a particular area of the country, such as Silicon Valley, that area should be placed off limits to that country.

East European governments do not always require that U.S. officials make travel arrangements through a central government office. Realistically, however, in that part of

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



the world the security police know about virtually every aspect of American official travel. In an open society like ours, the imposition of a requirement to make travel reservations through the Foreign Missions Office is surely consistent with the principle of reciprocity.

d. Regulation of Foreign-Controlled Commercial Entities

The Foreign Missions Act applies not only to diplomatic establishments such as embassies and U.N. missions, but also to state trading organizations and other entities that perform governmental functions. There is, once again, clear counterintelligence information establishing that Soviet and Warsaw Pact trading companies and other commercial entities in the U.S. controlled by those countries are engaged in espionage-related activities. There are two avenues to pursue in regulating their operations.

First, the Export Administration Act as adopted earlier this year authorizes the Commerce Department to require a license for transfer of controlled goods or technology to an embassy or other "affiliate" of a Communist government in the United States. This language should be applied by the Commerce Department to commercial entities that are owned or controlled by Communist governments and that may be used to transfer technology abroad surreptitiously.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Second, the Foreign Missions Act requirements should be applied to these same entities. Under the law as it now stands, such requirements clearly can be applied to state trading organizations such as the Soviet company AMTORG. It is more difficult, however, to apply the Foreign Missions Act to other Soviet bloc-controlled businesses. To close this gap, legislation should be enacted to amend the Foreign Missions Act and authorize the State Department to apply its requirements to "affiliates" of foreign governments, with the same meaning as in the Export Administration Act. A bill for this purpose will be introduced shortly.

These four steps -- equalizing U.S. and Soviet embassy and consular personnel, reducing the size of the Soviet U.N. Mission, requiring Foreign Mission Office travel controls for Warsaw Pact country representatives, and regulating foreign-controlled commercial entities -- are necessary to implement a national counterintelligence strategy. These hearings before the Permanent Subcommittee on Investigations will perform a vital function by letting the American public and all elements of the Executive branch know why such measures are necessary and how strongly they are supported in the Congress.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

WILLIAM S. COHEN MAINE
ORRIN HATCH UTAH
FRANK MURKOWSKI ALASKA
ARLEN SPECTER PENNSYLVANIA
CHIC HECHT NEVADA
MITCH MCCONNELL KENTUCKY

SAM NUNN GEORGIA
THOMAS F. EAGLETON MISSOURI
ERNEST F. HOLLINGS SOUTH CAROLINA
DAVID L. BOREN OKLAHOMA
BILL BRADLEY NEW JERSEY

ROBERT DOLE KANSAS, EX OFFICIO
ROBERT C. BYRD WEST VIRGINIA, EX OFFICIO

BERNARD F. MCMAHON, STAFF DIRECTOR
ERIC D. NEWSOM, MINORITY STAFF DIRECTOR

# United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510

Executive Registry
85- 3078

June 20, 1985

The President
The White House
Washington, D.C. 20500

Dear Mr. President:

Earlier today, I was asked to lead the opposition to a proposal by Senator Byrd and others to establish a National Commission on Security and Espionage. Such a Commission would have had four members appointed by the Congress and four by the President. We who opposed the proposal prevailed by a 50-48 margin.

I accepted the task of opposing the Byrd amendment because of a strong belief that the proposal would delay action on this immediate and serious problem for at least 18 months and probably longer. We are all committed to move as quickly as possible -- and that is most appropriately done within the existing structure. A crucial element in my conviction that we can make the current system respond quickly was the informal commitment that I had received from the Administration to full and complete support for the Senate Intelligence Committee's current study of the Soviet intelligence threat and U.S. counterintelligence and security programs.

It will be helpful to the Committee to have your personal commitment to Administration support of our enterprise, at each stage: determining how best to examine the problem; jointly developing recommendations; and ensuring implementation of improvements. Such an explicit commitment will not only facilitate the work of the Committee, but also help us when the Byrd proposal is raised again, which is quite likely.

You and we share an historic opportunity -- both to dramatically improve U.S. counterintelligence and

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



security and to demonstrate how Congress and the Executive can work together to achieve progress in sensitive intelligence areas. With your firm support, I am sure we can accomplish much indeed.

Sincerely,

Dave Durenberger
Chairman

cc: The Honorable George P. Shultz
The Honorable Caspar W. Weinberger
The Honorable Edwin Meese, III
The Honorable William Webster
The Honorable William J. Casey

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

WILLIAM V. ROTH, JR. DELAWARE
WILLIAM S. COHEN MAINE
ORRIN HATCH UTAH
FRANK MURKOWSKI ALASKA
ARLEN SPECTER PENNSYLVANIA
CHIC HECHT NEVADA
MITCH MCCONNELL KENTUCKY

LLOYD BENTSEN TEXAS
SAM NUNN GEORGIA
THOMAS F. EAGLETON MISSOURI
ERNEST F. HOLLINGS SOUTH CAROLINA
DAVID L. BOREN OKLAHOMA
BILL BRADLEY NEW JERSEY

ROBERT DOLE KANSAS EX OFFICIO
ROBERT C. BYRD WEST VIRGINIA EX OFFICIO

BERNARD F. MCMAHON STAFF DIRECTOR
ERIC D. NEWSOM MINORITY STAFF DIRECTOR

# United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510

Executive Registry
85- 3078 /2

July 16, 1985

The Honorable William V. Roth
The Honorable Thomas F. Eagleton
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Bill and Tom:

Senator Byrd's bill to establish a National Commission on Security and Espionage has been referred to the Committee on Government Affairs, and I think he deserves to be told what the Select Committee on Intelligence has done in this area since his proposal was debated on the floor last month.

Members of the Select Committee clearly share Senator Byrd's concern regarding the need for action to improve the counterintelligence and security programs of the United States. Early this year, Members agreed that a review of these programs should be high on our list of priorities. The Walker and Scranage cases, the Miller trial in Los Angeles and the work of the Permanent Subcommittee on Investigations have also underlined the need for attention to this subject.

The Select Committee has followed recent counterintelligence cases, keeping in mind the need to do nothing that would jeopardize current investigations or prosecutions. We also had a most enlightening closed session on security at the U.S. Embassy in Moscow. We will continue formal hearings on the subject this week with a closed session on the hostile intelligence threat. Witnesses from the CIA and the FBI will make that presentation this Thursday at 4:30 p.m. in room SH-219 following our weekly intelligence update from DIA. Next Tuesday we will breakfast with Admiral Bobby Inman, whose commission on the security of U.S. facilities overseas recently submitted a report to the Secretary of State on security against technical penetrations.

COMMITTEE SENSITIVE

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

STAT
Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Page Denied

Next 4 Page(s) In Document Denied

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

WILLIAM S. COHEN, MAINE
ORRIN HATCH, UTAH
FRANK MURKOWSKI, ALASKA
ARLEN SPECTER, PENNSYLVANIA
CHIC HECHT, NEVADA
MITCH McCONNELL, KENTUCKY

SAM NUNN, GEORGIA
THOMAS F. EAGLETON, MISSOURI
ERNEST F. HOLLINGS, SOUTH CAROLINA
DAVID L. BOREN, OKLAHOMA
BILL BRADLEY, NEW JERSEY

ROBERT DOLE, KANSAS, EX OFFICIO
ROBERT C. BYRD, WEST VIRGINIA, EX OFFICIO

BERNARD F. McMAHON, STAFF DIRECTOR
ERIC D. NEWSOM, MINORITY STAFF DIRECTOR

# United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510

#85-4219

December 13, 1985

Dear Colleague:

As the first session of the 99th Congress comes to an end, we want to bring you up to date on the comprehensive review of counterintelligence and security programs that the Select Committee is conducting. We know you share our concern about the upsurge in espionage cases during 1984-85 and the questions they raise about the adequacy of measures to protect national secrets. The Committee worked intensively this year to identify and begin to remedy deficiencies in U.S. defenses against hostile intelligence operations.

At the beginning of this Congress, we decided that the Committee should make an independent assessment of counter-intelligence and security programs. We advised the Administration of our plans in the spring, and we announced them publicly on June 11. Our guiding principle from the outset has been to cooperate as closely as possible with the Executive branch. We consult regularly with the National Security Council staff, and the President has designated senior officials to represent the Administration at a series of closed hearings. Our objective is to reach agreement with the Administration on a common agenda for immediate actions and long-range decisions.

The Committee held two types of closed hearings on counterintelligence and security matters this year. The first addressed specific needs or cases, while the second reviewed the full range of policies and programs.

We started the hearings on specific needs with a session in March on counterintelligence requirements in the Intelligence Authorization Act for FY 1986. Another hearing examined the need for greater controls over the numbers and activities of hostile intelligence officers in this country. The Committee approved a proposal by Senators Leahy and Cohen to establish a policy of equivalence in the numbers of U.S. and Soviet embassy and consular personnel, as well as Senator Roth's proposal to control travel by Soviet bloc nationals working for the United Nations Secretariat. Both the Leahy-Cohen amendment and the Roth amendment were later enacted in the State Department Authorization Act. The Committee also issued a public report, prepared with the Intelligence Community's assistance, on the "Soviet Presence in the U.N. Secretariat."

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



In June, the Committee looked at the damage done by the Walker family and Whitworth espionage network and the security and counterintelligence shortcomings revealed by their years of work as Soviet agents. Another hearing covered the security situation at the U.S. Embassy in Moscow, including both technical security and vulnerabilities resulting from employment of a large number of Soviet nationals. Shortly thereafter, the Inman Panel submitted to the Committee a classified annex to its report on security problems at U.S. facilities overseas. At a subsequent session, the Committee considered resource requirements for improved security countermeasures abroad; we thereupon proposed what became a $35 million supplemental appropriation for this purpose.

In the fall, the Committee received several briefings on Edward Lee Howard, the former CIA officer who apparently fled the country before he could be arrested on espionage charges. In addition, the Committee conducted preliminary hearings on the Yurchenko defection and the Pollard, Chin, and Pelton espionage cases. We have requested and are awaiting detailed assessments of the counterintelligence, security, and management implications of the Howard and Yurchenko cases.

While these hearings were necessary and useful, they were not sufficient to make a comprehensive assessment of U.S. counterintelligence operations and security practices. Therefore, the Committee held another series of closed hearings to consider these matters more systematically. We began in July with a survey by the FBI and CIA of the full scope of the hostile intelligence threat, both human and technical. In the fall, the Director of Central Intelligence and other senior officials described the Administration's actions to improve counterintelligence capabilities and security measures. At a later hearing on counterintelligence capabilities and requirements into the 1990s, the FBI Director and senior counterintelligence officials from the CIA and DoD discussed improvements underway and planned to upgrade worldwide counterintelligence operations and analysis.

The next hearing focused on personnel and information security. General Richard Stilwell presented the report of the DoD Security Review Commission, which calls for significant reforms in the security policies of Defense agencies, contractors, and the military services. At the same hearing the Director of the Information Security Oversight Office solicited the Committee's input on thirteen recommendations being submitted to the NSC to discourage overclassification,

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



control overdistribution of classified information, improve classification management, enforce the need-to-know principle, and reduce unauthorized disclosures.

The most recent of these hearings covered communications and computer security and technical surveillance countermeasures. Witnesses were the Deputy Director of Central Intelligence; the Assistant Secretary of Defense for Command, Control, Communications and Intelligence; the Director of the State Department's Bureau of Diplomatic Security; and officials from NSA and CIA. Another hearing in this series is scheduled for early next year.

The Committee is now pulling together the results of these hearings with the aim of working with the NSC on an agreed agenda. We have just made several recommendations to the National Security Council regarding information security and we have encouraged prompt action on initiatives proposed by the Information Security Oversight Office. A copy of our recommendations is enclosed. (Other appropriate committees have also been asked for their input to the Administration.)

In October we issued a joint statement describing the Intelligence Committee's work and recommending specific measures to control the hostile intelligence presence in this country. We also outlined two fundamental objectives we hope to accomplish. First is development by the Executive branch, with appropriate Congressional input, of a national counterintelligence strategy. Second is formulation of a comprehensive National Strategic Security Program to provide coherent and balanced policy guidance for all aspects of the protection of information and activities that have the greatest strategic importance. A copy of this statement, which was presented at a public hearing of the Governmental Affairs Committee's Permanent Subcommittee on Investigations, is also enclosed.

We believe the lesson of this "year of the spy" is that the Administration and Congress must work closely together to reach a common understanding of the nature of the threat and to make substantial improvements in U.S. counterintelligence and security programs. The Intelligence Authorization Act for FY 1986 requires the President to submit to the Intelligence Committees within 120 days a classified report on the policies and programs needed to protect U.S. Government information and activities from the hostile intelligence threat. After we

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



receive this report next spring, the Committee will report to the Senate. Early next year we also expect to propose specific legislative and budgetary initiatives to be adopted before the end of the 99th Congress.

As we complete these efforts, we solicit your views and proposals so that the Committee can have the benefit of the best thinking in the Senate on these problems. Finally, as we conclude a very difficult year, we want to express our deep appreciation to all the Members of the Committee and to other Members of the Senate who have given us their support and encouragement. We will continue to pursue these issues until major improvements have been adopted and implemented.

Sincerely,

Dave Durenberger
Chairman

Patrick J. Leahy
Vice Chairman

Attachments

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

DAVE DURENBERGER, MINNESOTA, CHAIRMAN
PATRICK LEAHY, VERMONT, VICE CHAIRMAN
WILLIAM V. ROTH, JR., DELAWARE
WILLIAM S. COHEN, MAINE
ORRIN HATCH, UTAH
FRANK MURKOWSKI, ALASKA
ARLEN SPECTER, PENNSYLVANIA
CHIC HECHT, NEVADA
MITCH McCONNELL, KENTUCKY
LLOYD BENTSEN, TEXAS
SAM NUNN, GEORGIA
THOMAS F. EAGLETON, MISSOURI
ERNEST F. HOLLINGS, SOUTH CAROLINA
DAVID L. BOREN, OKLAHOMA
BILL BRADLEY, NEW JERSEY
ROBERT DOLE, KANSAS, EX OFFICIO
ROBERT C. BYRD, WEST VIRGINIA, EX OFFICIO
BERNARD F. McMAHON, STAFF DIRECTOR
ERIC D. NEWSOM, MINORITY STAFF DIRECTOR

United States Senate
SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510

#85-4252

December 13, 1985

The Honorable Robert C. McFarlane
Assistant to the President for
National Security Affairs
The White House
Washington, D.C. 20500

Dear Bud:

On November 29, 1985, Mr. Steven Garfinkel, Director of the Information Security Oversight Office, advised the Select Committee that he expected action early next year on the initiatives he has recommended to improve the Government-wide information security system. Mr. Garfinkel discussed these proposals with the Committee at a hearing on November 20 and indicated that the National Security Council would like to have our input on these or other initiatives the Committee might propose.

Attached are the Committee's recommendations on information security in response to Mr. Garfinkel's invitation. We appreciate the opportunity to comment on his proposals, and we are grateful for the excellent cooperation we have received from the Executive branch on all aspects of our review of counterintelligence and security programs. We look forward to continuing to work with the NSC staff on an agenda for immediate action and long-range decisions in this area.

Sincerely,

Dave Durenberger
Chairman

Patrick Leahy
Vice Chairman

Attachment

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

# SENATE SELECT COMMITTEE ON INTELLIGENCE
# RECOMMENDATIONS ON INFORMATION SECURITY

The Director of the Information Security Oversight Office (ISOO) has recommended a series of initiatives to improve the Government-wide information security system. They reflect a well-founded concern about five problems: overclassification or unnecessary classification; over-distribution of classified information; inadequate classification management; erosion of the need-to-know principle; and unauthorized disclosure. The ISOO recommendations were developed in consultation with the agencies most involved with national security information, and they parallel several points made by the DoD Security Review Commission. The Select Committee on Intelligence has reviewed the ISOO recommendations and submits the following proposals.

## 1. Background

The Select Committee has a long-standing interest in the information security system. The Committee provided input to the Administration in 1977 and in 1982 on the succeeding Executive Orders on National Security Information. The Committee's report on "National Security Secrets and the

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



Administration of Justice" led to enactment of the Classified Information Procedures Act of 1980, which set procedures for minimizing unnecessary disclosure of national security secrets in criminal prosecutions. The Intelligence Identities Protection Act and the CIA Information Act were both enacted with Committee support so as to improve protection of vital intelligence sources and methods. In each instance, the Committee sought to strike a balance between legitimate interests in secrecy and disclosure.

The upsurge in espionage cases during 1984-85 has focused more attention on weaknesses in information security policy. The cases have highlighted the security problems that result, in large measure, from attempting to protect too much and thereby stretching personnel and other security programs too thin. The issue is not just inadequate resources, but attitudes as well, and the concerns date back many years. No one has characterized the situation better than the late Justice Potter Stewart, who wrote in the Pentagon Papers Case in 1972:

> I should suppose that moral, political, and practical considerations would dictate that the very first principle ... would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



> intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.

Concern about failure to meet these standards is widespread in and out of government.

During the past year, the Committee has been undertaking a comprehensive review of counterintelligence and security policies of the United States. This review has included not just highly-publicized espionage cases and other specific security problems, but the full range of counterintelligence efforts and security programs designed to protect sensitive information and activities from hostile intelligence operations. In this context, the Committee has taken a careful look at information security policy and its relationship with other security disciplines (personnel, physical, communications, computer, and technical security) as well as with counter-intelligence programs. The Committee's recommendations are being submitted to the Assistant to the President for National Security Affairs as part of continuing consultations between the Committee and the NSC, with the aim of reaching agreement on an agenda for immediate actions and long-range decisions to improve U.S. counterintelligence and security programs.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



2. Immediate Implementation

The Committee believes the ISOO recommendations are an excellent agenda for short-term actions to improve the information security system, although as noted below the Committee has several additional proposals for long-range decisions. Other recommendations that require prompt action at the departmental or national level include many of those contained in the Stilwell Commission report, the Inman Panel's classified annex on overseas technical security, and the latest National Assessment of the Hostile Intelligence Services Threat and U.S. Countermeasures. The Committee supports the President's recent action to establish a new interagency committee, chaired by a member of the NSC staff, to ensure effective action on recommendations to control the hostile intelligence presence and to improve security awareness programs. Strong leadership is essential to carry out effectively the recent legislation on controlling travel by Soviet bloc nationals at the UN Secretariat and on equivalence between U.S. and Soviet official representation. The NSC should promptly address other pending counter-intelligence and security recommendations, including the ISOO recommendations, and assign responsibilities for implementation.

The ISOO recommendations themselves are carefully drafted to tighten the administration of the current

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



classification system. Even if more fundamental changes are needed, as the Committee believes, they should not be an excuse for delay. Especially important are the revisions proposed in Executive Order 12356 to require the reporting of improper classification, to require agency heads to ensure personal accountability for management of classified information, and to require effective internal oversight and periodic reconfirmation of special access programs.

These revisions, along with the other directives and policy changes recommended by ISOO, should have the strong, publicly-stated endorsement of the President and the principal members of the National Security Council. The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, and the Assistant to the President for National Security Affairs should make clear to their subordinates, publicly where appropriate, their commitment to the new information security policies for curbing overclassification and overdistribution, improving classification management, enforcing the need-to-know principle, and improving security awareness and investigations of unauthorized disclosures. They should hold senior executives and program managers personally responsible for effective implementation.

3. National Strategic Security Program

The Committee's review of counterintelligence and

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



security policies in this "year of the spy" has found troublesome evidence of a lack of overall national policy guidance, especially with regard to the security programs and countermeasures that are supposed to protect classified information. The Committee believes there is a need for a comprehensive and integrated National Strategic Security Program to coordinate and foster the protection of information and activities having the greatest strategic importance. This does not mean establishing a counterintelligence "czar" or taking from individual agencies and officials their responsibility for implementing national policies as they affect their work. Rather, the NSC's statutory mandate to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security gives it the responsibility to ensure coherent national policy direction and implementation for:

- o Information security and classification
- o Personnel security
- o Telecommunications and computer security
- o Technical surveillance countermeasures
- o Physical security
- o Industrial security
- o Research and development efforts
- o Security awareness requirements.

To assist the NSC, a single body should be assigned responsibility for policy planning and analysis of all aspects of strategic security. In addition, there must be more effective coordination among the various

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



overlapping forums that now share responsibility for security policy, including the DCI's Security Committee, the National Telecommunications and Information Systems Security Committee, and the Interagency Group-Countermeasures.

This is not an entirely new concept. The need for national policy guidance was identified in 1957 by the Commission on Government Security, whose Vice Chairman was Senator John Stennis. It proposed an office to ensure greater uniformity and higher quality for personnel and industrial security throughout the government. Earlier this year, the Chairman and Ranking Minority Member of the Senate Permanent Subcommittee on Investigations, Senators Roth and Nunn (who also serve on the Select Committee), recommended establishment of an executive body with Government-wide personnel security oversight responsibilities similar to those which the ISOO now has for information security.

The DoD Security Review Commission emphasized a similar need within the Defense Department. The Stilwell Commission stressed "that all security disciplines have as their fundamental purpose the protection of classified information and must be applied in a fully balanced and coordinated way." Thus, the Commission urged the Secretary of Defense to consider placing related security

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



policy responsibilities in a single OSD staff element, with the Defense Security Institute having an expanded policy support mission. (The ISOO recommendations call for the DSI to have a Government-wide role in basic training for all Executive branch security personnel.)

The Stilwell Commission's idea makes sense at the national level as well. The NSC should assign to an appropriate body the task of putting together a fully balanced and coordinated National Strategic Security Program for protecting the most sensitive information and activities. A senior official should be designated to testify on the National Strategic Security Program before the appropriate Committees of the Congress.

4. Streamlining the Classification System

The information security system requires more extensive reform than would result from the ISOO initiatives. While they would clearly help, the recommendations are based on the premise that, as Mr. Garfinkel stated to the Committee, the current structure is "fundamentally sound and, for the most part, works quite well." The Committee disagrees.

The Stilwell Commission reported that "too much information appears to be classified and much at higher levels than is warranted." It found that little scrutiny is given to classification decisions "out of ignorance or expedience" and that "few take the time to raise

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



questionable classifications with originators." Like Mr. Garfinkel, however, General Stilwell saw the problems as "primarily a matter of inadequate implementation of existing policy, rather than a matter of deficient policy."

The Committee shares the view of information security experts who see a fundamental, underlying problem in the complexity of the system. There are at least four levels of classification. Overlaying the three levels prescribed by Executive Order -- Confidential, Secret, and Top Secret -- is a complicated set of special access programs developed by various departments and agencies. The proliferation of special access programs is testimony to the failure of the current classification system. Mr. Garfinkel testified that "a number of these programs are probably unnecessary," and the Stilwell Commission reported that some special access programs actually afford less security protection than ordinary classification requirements.

If the classification system is to work in practice, it must be streamlined so that officials better understand their responsibilities. The Committee supports the ISOO and Stilwell Commission recommendations to require, rather than simply permit, challenges to classification believed to be improper. The impact will be limited, however, unless the classification rules are simplified.

The Committee recommends consideration of a two-level

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



system, based essentially on the current Secret-level standard and the Sensitive Compartmented Information (SCI) model used in the Intelligence Community. The Confidential classification should be dropped, as recommended nearly thirty years ago by the Commission on Government Security. In its 1957 report, the Commission observed that the danger of access to Confidential-level information was "not significant" and that the minimal clearance requirements for such access afforded "no real security check."

Whatever the legal formula for classification, the threshold should reflect a policy that classifies information only where truly necessary to maintain national security. As stated recently by General Eugene F. Tighe, former Director of DIA, "[I]f the U.S. security system for handling classified material is to be useful, only data that are critical to the United States' status as a political, economic and military power should be classified." The initial decision should be whether the information requires protection in order to prevent substantial harm to identifiable national security interests. Rather than assuming that information is classified, the burden should be to show the need for secrecy.

The other standard should focus on the much smaller universe of data that requires special protective measures above and beyond the normal safeguards for classified information. As is the case with intelligence data classified

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



SCI, classification at the second level should be based on a full analysis of the risks of compromise. Such analysis should ensure that special protective measures are imposed only where necessary and are not diluted by applying them too widely. Careful analysis should also provide the elements for more effective security briefings that help senior policy-makers as well as lower level employees understand the consequences of a security breach.

In the long run, simplifying the classification system will give the ISOO recommendations a much greater chance of reversing the natural incentives to overclassification and enforcing the need-to-know principle.

5. Disclosure Procedures

Disclosure of classified information to the news media raises a different set of issues. The Committee is especially concerned about leaks that compromise sensitive intelligence sources and methods. Such leaks will continue unless something is done about the underlying attitudes that foster disrespect for the rules of secrecy.

The Committee endorses the ISOO recommendation that new educational materials, both classified and unclassified, be developed to address the damage caused by unauthorized disclosures. More effective unclassified materials are especially important. The Committee has found the security orientation briefings offered routinely by the Executive

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



branch fall short of minimal requirements, even though some security officials can do an excellent job of explaining the significance of classification and compartmentation policies.

Even more important than education, however, are the procedures for authorized disclosure of classified information to the news media. The ISOO recommendation for reassessment of the policies for leak investigations may accomplish little without adequate controls over authorized disclosures. Currently, the practice of non-attributable background statements, often drawing on classified information, is pervasive. Such statements are virtually indistinguishable from leaks. They divert the overworked investigators of leaks from the cases in which administrative discipline, dismissal, or legal action is possible; and they reinforce the climate of cynicism that leads to leaks and counterleaks.

Senior officials who authorize disclosures of classified information on background, without permitting attribution to the source, gain two advantages that undermine an effective information security system. First, they often can conceal their responsibility for the disclosure, just as the leaker does. Second, they can avoid giving the originating agency a chance to argue against disclosure and explain the harm it would do. If the same information disclosed "on background" were contained in a press release, it would have to be formally declassified. In practice, however, classified information

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



authorized for disclosure on background technically remains classified. There may well be valid reasons for retaining a "background" briefing's classified character; but any serious effort to address the problem of leaks clearly must confront this practice and bring it under control.

Therefore, one of the most important actions to deter leaks and to change the atmosphere that promotes leaks would be to require, by Executive order, that agreed procedures be followed whenever any official authorizes disclosure of classified information to the news media. The procedures should apply not only to formal statements for attribution, but also to disclosures on background. They should require either that the information be declassified or that a record be maintained for purposes of accountability when authority is exercised or granted to disclose to the news media information that remains classified. Such procedures should include the requirements to consult the agency that originated the information and to designate the officials permitted to exercise or grant this authority.

Strong leadership is needed to break through the cycle of leak and counter-leak that pervades the policy community and jeopardizes highly sensitive intelligence sources and methods. The time is ripe to face the realities of press-government relations and adopt sensible rules that bring some order to the chaos that has fostered disrespect for

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



security.

6. Conclusion

The ISOO recommendations can make an important contribution to national security if they are implemented vigorously with high-level support. The Committee believes they should become part of a National Strategic Security Program that is monitored by the NSC and the Congress. They should also lead to more fundamental reforms to simplify the classification system and to establish procedures with consultation and accountability for authorized disclosures. These initiatives, together with actions in other areas of counterintelligence and security that the Committee is considering, can ensure a level of protection for sensitive information and activities commensurate with the threats and vulnerabilities the United States will face in the years ahead.

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

CONFIDENTIAL

The Director of Central Intelligence

Washington D C 20505

ICS 85-6099
20 December 1985

MEMORANDUM FOR: Members, Senior Interagency Group - Intelligence

SUBJECT: Counterintelligence Capabilities Improvements Report

As we discussed at last Tuesday's meeting, the Intelligence Authorization Act (Section 402) requires that the President submit to the HPSCI and SSCI, with 120 days, a full report (with an interim report due within 60 days) on "the capabilities, programs, and policies of the United States to protect against, detect, monitor, counter, and limit intelligence activities by foreign powers, within and outside the United States, directed at United States Government activities or information, including plans for improvements which are within his authority to effectuate and recommendations for improvements which are not within his authority to effectuate."

I have asked General Richard Stilwell to oversee the preparation of this report. He will be supported by the Community Counterintelligence Staff.

This is a very important undertaking, both for the Community and for our relations with the Congress, and, therefore, deserves priority action by the SIG(I). Accordingly, I ask that you give General Stilwell your fullest cooperation.

Please provide the names of your personal representative to work on this report to [redacted] Chief, CCIS, no later than Friday, 27 December 1985. 25X1

William J. Casey
Chairman,
Senior Intelligence Group - Intelligence

[redacted] 25X1

CONFIDENTIAL

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8



REFERENCE

Intelligence Authorization Act for Fiscal Year 1986

"COUNTERINTELLIGENCE CAPABILITIES IMPROVEMENTS REPORT

"Sec. 402. (a) Within 120 days after the date of enactment of this Act, the President shall submit to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report on the capabilities, programs, and policies of the United States to protect against, detect, monitor, counter, and limit intelligence activities by foreign powers, within and outside the United States, directed at United States Government activities or information, including plans for improvements which presently are within the authority of the executive branch to effectuate, and recommendations for improvements which would require legislation to effectuate. (U)

"(b) The report described in subsection (a) of this section shall be exempt from any requirement for publication or disclosure." (U)

C

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8

OVERALL FUNCTIONS AND MILESTONES

FUNCTIONS/SUBFUNCTIONS

MILESTONES

| | January | | February | | | | March | | | | | April | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 20-24 | 27-31 | 3-7 | 10-14 | 17-21 | 24-28 | 3-7 | 10-14 | 17-21 | 24-28 | 31-4 | 7-11 | 14-18 | 21-25 | 28-2 |
| Distribute initial advisement | 20 — 24 | | | | | | | | | | | | | | |
| Review selected SSCI hearings and related correspondence | 22 — 27 | | | | | | | | | | | | | | |
| Review content of SSCI interim report (findings of hearings) | 22 — | — 31 | | | | | | | | | | | | | |
| Acquire and develop executive branch input (task, draft) | 23 — | — | 4 | | | | | | | | | | | | |
| Synthesize SSCI report and executive branch input (analyze, examine, structure) | 23 — | — | — | 14 | | | | | | | | | | | |
| Produce executive branch interim report (write and coordinate) | | 31 — | — | 14 | | | | | | | | | | | |
| Executive branch review and approval | | | 14 — | 17 | | | | | | | | | | | |
| Consult with Congressional staffs | | | | 17 — | 21 | | | | | | | | | | |
| Produce executive branch final report | | | | | 24 — | — | 10 | | | | | | | | |
| Coordinate final report through SIG-I system | | | | | | | 10 — | 14 | | | | | | | |
| Submit final report to SSCI | | | | | | | | 17 — | 21 | | | | | | |
| SSCI submits final report to Congress | | | | | | | | | | | | | | | |

1

Sanitized Copy Approved for Release 2011/07/06 : CIA-RDP88G01116R000400390017-8